Security Hub Partner FAQs

1. What are the benefits of Security Hub integration?
    a. Customer satisfaction. The number one reason to integrate with Security Hub is because you have customer requests to do so. Security Hub is the security and compliance center for AWS customers and is designed as the first stop where AWS-focused security and compliance professionals will go each day to understand their security and compliance state. Listen to your customers. They will tell you if they want to see your findings in Security Hub.
    b. Discovery opportunities. We promote partners with certified integrations inside the Security Hub console, including links to their Marketplace listings. This is a great way for customers to discover new security products.
    c. Marketing opportunities. Vendors with approved integrations can participate in webinars, press releases, create slick sheets, and demonstrate their integrations to AWS customers.

2. What types of partners are there?
    a. Partners that push findings to Security Hub
    b. Partner that receive findings from Security Hub
    c. Partners that do both a and b
    d. Consulting partners that assist customers with setting up, customizing, and using Security Hub in their environment

3. How does a partner integration with Security Hub work at a high-level?
    a. Partners gather findings from within a customer account or from their own AWS account, transform the format of the findings to the AWS Security Finding Format (ASFF), and push those findings to the appropriate Security Hub regional endpoint. Partners may also receive findings from Security Hub via CloudWatch Events.
4. What are the basic steps for completing an integration with Security Hub?
    a. Submit your partner manifest information.
    b. Receive Product ARNs to use with Security Hub, if you will be sending findings to Security Hub.
    c. Map your findings to ASFF.
    d. Define your architecture for sending/receiving findings to/from Security Hub.
    e. Create a deployment framework for customers (e.g., CloudFormation scripts).
    f. Document your setup/configuration instructions for customers.
    g. Define any custom insights (aka correlation rules) that customers can use with your product.

    h. Demo your integration to the Security Hub team.
    i. Submit marketing information for approval (website language, press release, architecture slide, video, slick sheet)

5. What is the process for submitting the partner manifest? AWS services to send findings to Security Hub?
    a. You can submit the manifest information to the Security Hub team via securityhub-partners@amazon.com. You will be issued product ARNs within 7 calendar days.

6. What types of findings should I send to Security Hub?
    a. One of Security Hub's pricing dimensions is based on the number of findings ingested. As a result, partners should refrain from sending findings that don't provide value to customers. For example, some vulnerability management vendors only send findings with a CVSS score of 3 or above (out of a possible 10).

7. What are the different approaches for partners to send findings to Security Hub?
    a. There are two primary approaches:
        i. Partners send findings from their own designated AWS account using the BatchImportFindings API.
        ii. Partners send findings from within the customer account using the BatchImportFindings API. This could be via Assume Role approaches, but they are not required.

8. How do partners gather their findings and push them to a Security Hub regional endpoint?
    a. Partners have used different approaches for this, as it is highly dependent on the architecture of your solution. For example, some partners built a Python app that could be deployed as a CloudFormation script which gathers the partner's findings from within the customer environment, transforms them into ASFF, and pushes them to the regional endpoint. Other partners, have built out a full wizard that gives the customer a single-click experience to push findings to Security Hub.

9. How does a partner know when to start sending findings to Security Hub?
    a. We support partial batch authorization for the BatchImportFindings API, so that you can send all of your findings to Security Hub for all of your customers. If some of your customers haven’t yet subscribed to Security Hub, we will not ingest those findings, but we will ingest any authorized findings in the batch.

10. What are the steps that need to be completed to send findings to a customer's Security Hub instance?

a. Ensure the correct IAM policies are in place.
b. Enable a product subscription (i.e., resource policies) for that account(s) via the API (EnableImportFindingsForProduct) or UI on the partner page. This can be done by the customer or you acting on behalf of the customer using cross-account roles.
c. Ensure the ProductArn of the finding is your product's public ARN.
d. Ensure the AwsAccountId of the finding is the customer's account ID.
e. Ensure your findings don't have any malformed data according to the AWS Security Finding Format (e.g., required fields are populated, no non-allowed values, etc.)
f. Send findings to the correct regional endpoint in batches.

11. What IAM permissions must be in place for a partner to send findings?
    a. IAM policies must be configured for the IAM user/role calling BatchImportFindings (or other API calls). The easiest test is to do this from an admin account. You can constrain these down to action: 'securityhub:BatchImportFindings' and resource: the productArn and/or the productSubscriptionArn. Resources in the same account can be configured with IAM policies without requiring resource policies.
    b. To rule out IAM policy issues from the caller of BatchImportFindings, have them set the IAM policy to:
        i. {
            Action: 'securityhub:*',
            Effect: 'Allow',
            Resource: '*'
            }
    c. Be sure to check that there are no "deny" policies for the caller anywhere. Once you get it working with that, you can restrict it down to:
        i. {
            Action: 'securityhub:BatchImportFindings',
            Effect: 'Allow',
            Resource:
        'arn:aws:securityhub:<region>:<account>:product/mycompany/myproduct'
        },
        {
            Action: 'securityhub:BatchImportFindings',
            Effect: 'Allow',
            Resource: 'arn:aws:securityhub:<region>:*:product-subscription/mycompany/myproduct'
        }

12. What is a product subscription?

a. In order to receive findings from a specific partner/product, the customer (or the partner with cross-account roles working on behalf of the customer) must put in place a product subscription via the UI in the Settings/Partner page or API via the EnableImportFindingsForProduct API call. The product subscription creates a resource policy that authorizes the findings from the partner to be received (or sent) by the customer. See the document on "Security Hub Resource Policy Approach" for details.
b. We have two types of resource policies for partners: BATCH_IMPORT_FINDINGS_FROM_PRODUCT_ACCOUNT and BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT. During the partner onboarding process, you can request to receive either one or both. With the PRODUCT_ACCOUNT one, you can only send findings to SecHub from the account listed in your product ARN. With the CUSTOMER_ACCOUNT one, you can only send findings from the customer account that subscribed to you.

13. Assume a customer created a Master account and added a few member accounts, do they need to subscribe to the partner to each of the member accounts? Or, can they just subscribe from Master account, and the partner can then send findings against resources in all member accounts. The driver behind this question is whether the permissions get created for all member account, just based on Master account registration.
    a. The partner needs to make sure that a product subscription is put in place for each account. That can be done programmatically through the API.

14. What is my product ARN?
    a. Your product ARN is your unique identifier that SH generates for you and that you use to submit findings. You receive a product arn for each product that you integrate with Security Hub. The correct product ARN must be part of every finding that you send to Security Hub or those findings will be dropped. It consists of the following format: arn:aws:securityhub:[region code]:[account number]:product/[company name]/[product name]. For example:

        i. arn:aws:securityhub:us-west-2:222222222222:product/generico/secure-pro
    b. You are given product ARNs for each region where Security Hub is deployed. The account number, company, and product names are dictated by your partner manifest submissions. You never change any of the information associated with your product ARN except for the region code to match the region you are submitting findings for. A common mistake that some partners have made is to change the account number to match the account where you are currently working from. The account number does not change. You submit

a "home" account number as part of the manifest submission and this is the account number that is locked as part of your product ARN.

c. When Security Hub launches in new regions, ARNs for your products will be automatically generated for those regions using standards region codes.
d. Every account is also automatically provisioned a private product ARN. You can use this to test importing findings within your own development account prior to being issued your official public product ARN.

15. What format should be used to send findings to Security Hub?
    a. Findings must be provided in the AWS Security Finding Format (ASFF):
        i. Public docs: https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-findings-format.html
        ii. The expectation is that all the information in partner's native findings is fully reflected in the ASFF. There are custom fields like the ProductFields and Resource.Details.Other that allow partners to map data that doesn't neatly fit in a predefined fields.

16. What is the right regional endpoint to use?
    a. Partners must send findings to the Security Hub regional endpoint associated with the customer account.

17. Where can I find the list of regional endpoints?
    a. https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-regions.html

18. Can I submit cross-region findings?
    a. Security Hub does not yet sub cross-region submission of findings for the native AWS services (e.g., GuardDuty, Macie, Inspector), but if your customer allows it, Security Hub does not prevent partners from submitting findings from different regions. In this sense, a partner can call a regional endpoint from anywhere, and the resource information of the ASFF doesn't have to match the region of the endpoint. However, the ProductArn must match the region of the endpoint.

19. What are the rules and guidelines for sending batches of findings?
    a. You can batch up to 100 findings or 240 kb in a single call of BatchImportFindings. Please queue up and batch as many findings as possible up to this limit.
        i. You can batch a set of findings from different accounts. However, if any of the accounts in the batch are not subscribed to Security Hub, the entire batch will fail. This is a

limitation of API Gateway's baseline authorization model. However, we have a roadmap item to improve this baseline experience and only fail on individual accounts/findings.

20. Can I send updates to findings that I created?
    a. Yes, if you submit a finding with the same product ARN and same finding ID, it will overwrite the previous data for that finding. Note that all the data will be overwritten, so you should submit a complete finding. Customers are metered and billed for both finding updates and new findings.

21. Can I send updates to findings that someone else created?
    a. Yes, if the customer grants you access to the BatchUpdateFindings API, you can update certain fields using that API. This API is designed to be used by customers, SIEMs, ticketing system, and SOAR platforms.

22. How are findings aged-off?
    a. Security Hub ages out findings 90 days after the last update date. After this time, the aged out findings will be purged from the Security Hub Elasticsearch cluster. If a partner updates a finding with the same finding ID, and it has been aged off, a new finding will be created in Security Hub. Customers can move findings out of SecurityHub via CloudWatch Events, which enables all findings to be sent to target(s) of the customer's choice. In general, we recommend that partners create new findings every 90 days and do not update findings forever.

23. What throttles does Security Hub put in place?
    a. Security Hub throttles GetFindings API calls, as the recommended approach to access findings is via CloudWatch Events. Security Hub does not implement any other throttling on internal services, partners, or customers beyond that enforced by API Gateway and Lambda invocations. There is a plan to implement throttles in the future via API Gateway tooling.

24. What is the timeliness or latency SLAs or expectations for findings being sent to Security Hub from source services?
    a. The aim is to be as near real time as possible for both initial findings as well as updates to findings. Partners should send findings to Security Hub within 5 minutes of them being created.

25. How can I receive findings from Security Hub?
    a. There are two methods for this:
        i. All findings are automatically sent to CloudWatch Events. A customer can create specific CloudWatch Event rules to send

findings to specific targets (e.g., a SIEM, a S3 bucket, etc.). Note: this capability replaced our legacy GetFindings API, which is significantly throttled.

ii. CloudWatch Events for custom actions. Security Hub allows customers to select specific findings or groups of findings from within the console and take action on them (e.g., send to a SIEM, ticketing system, chat platform, or remediation workflow). This would be part of an alert triage workflow that a customer is performing within Security Hub. These are called custom actions. When a user takes a custom action, a CloudWatch Event is created for those specific findings. A partner could leverage this capability and build out CloudWatch Event rules/targets for a customer to use as part of a custom action. Note that this capability is not for automatically sending all findings of a particular type or class to CloudWatch Events. It is for a user taking action on a specific finding(s).

b. A partner can use the custom action APIs (e.g., CreateActionTarget) to auto-create Action menu items associated with their product (e.g., via CloudFormation templates). You would also use CloudWatch Event rule APIs to create corresponding CloudWatch Event rules associated with the custom action. CloudWatch Event rules can also be created via CloudFormation templates to automatically ingest all findings or all findings with certain characteristics from Security Hub.

26. What are the requirements to become a MSSP partner?
    a. You must demonstrate how Security Hub is used as part of your service delivery to customers.
    b. You should have user documentation explaining your usage of Security Hub.
    c. If the MSSP is a findings provider, they must demonstrate sending findings to Security Hub.
    d. If the MSSP is only receiving findings from Security Hub, they must have a CloudFormation template at a minimum for setting up the appropriate CloudWatch Event rules.

27. What are the requirements to become a non-MSSP consulting partner?
    a. Consulting partners can become Security Hub partners. They should submit private two case studies on how they helped a specific customer do the following:
        i. Setup SecHub with IAM permissions needed by the customer
        ii. Assist in connecting already integrated ISV solutions to SecHub using the configuration instructions on the partner page in the console.
        iii. Assist customers in custom product integrations
        iv. Build custom insights relevant to customer needs/datasets

v. Build custom actions
vi. Build remediation playbooks
vii. Build Quickstarts that aligns to Security Hub's compliance standards; these must be validated by the Security Hub team.

b. Case studies do not need to be publicly shareable.

28. What are the requirements around how I deploy my integration with Security Hub with my customers?
    a. Integration architectures between Security Hub and partner products vary from partner to partner in terms of how that partner's solution is operated. All partners should ensure that the setup process for the integration takes no longer than 15 minutes. If the partner is deploying integration software into the customer's AWS environment, they should leverage CloudFormation templates to simplify the integration. Some partners have created a one-click integration, which is highly encouraged.

29. What are my documentation requirements?
    a. All partners are required to provide a link to their documentation that describes the integration and setup process/steps between their product and AWS Security Hub (including your usage of CloudFormation templates). That documentation should also include information on your usage of ASFF. Specifically, this should what ASFF finding types you are using for your different findings. If you have any default insight definitions, we recommend that you include them here as well.
    b. Other potential information to include is your use case for integration with Security Hub, average volume of findings sent, your integration architecture, what regions you do/don't support, latency between when findings are created and sent to Security Hub, and whether you update findings.

30. What are custom insights?
    a. Partners are encourage to define custom insights for their findings. Insights are lightweight correlation rules that help a customer prioritize which findings and resources most require attention and action. Security Hub has a CreateInsight API, so partners can create custom insights inside a customer account as part of their CloudFormation template. These insights will appear in the customer's console.

31. Can I submit dashboard widgets?
    a. No, not at this time. You can only create default insights.

32. What is your pricing model
    a. See https://aws.amazon.com/security-hub/pricing/

33. How do I submit findings to the Security Hub demo account as part of the final approval process for my integration?
    a. The account number is 068873283051 and it is in PDX (us-west-2). You can send findings to the Security Hub demo account using your provided productARN that includes us-west-2, and the findings should include our account number (068873283051) in the account number field of ASFF. Please do not send us any sensitive/PII data, as this data is used for public demos. By sending us this data, you authorize us to use it in demos.

34. What error or success messages does BatchImportFindings provide?
    a. Currently, Security Hub provides a response for auth and a response for BatchImportFindings. However, more crisp success/failure/error messages are being developed.

35. What error handling is the source service responsible for?
    a. Source services are responsible for all error handling, including handling error messages, retries, throttling, alarming, handling feedback/error messages sent through the Security Hub feedback mechanism.

36. What are some resolutions to common problems?
    a. I'm getting **AuthorizerConfigurationException**!" This is caused by either a malformed AwsAccountId or ProductArn. How to troubleshoot:
        i. AwsAccountId has to be 12, no more, no less, digits
        ii. ProductArn must be in the format: arn:aws:securityhub:<us-west-2 or us-east-1>:<accountId>:product/<company-id>/<product-id> (the accountId does not change from the one that the Security Hub team included in the product ARNs that were originally provided to the partner).
    b. I'm getting **AccessDeniedException**!" This is caused by either attempting to send to and/or from the wrong account or not having a ProductSubscription. The error message will contain and ARN with a resource type of "product" or "product-subscription". This error only occurs during cross-account calls. If they're calling BatchImportFindings with their own account for the same account in AwsAccountId and ProductArn, it's all IAM policies and has nothing to do with ProductSubscriptions.
    c. In general, be sure the customer account and product account that you're using are actually the registered accounts. Some partners have used an account number for the product (which is in the product ARN), but are trying to use an entirely different account to call BatchImportFindings. In other cases they've created ProductSubscriptions for other customer accounts (or even their own

product account), but not the customer account that they're attempting to import findings into.

37. Where do I send questions, comments, bugs?
    a. securityhub-partners@amazon.com

38. Which region do I send findings to for items related to global AWS services. For example, IAM related findings?
    a. Findings should be sent into the same region that the finding was detected in. For something like IAM it is very likely that the partner solution will find the same IAM issue in multiple regions. In this case the finding would be sent into every region that the issue was detected in. If the customer is running in three regions and the same IAM issue is detected when looking at all three regions then the finding should be sent to all three regions. When an issue is resolved the update to the finding should be sent into all the regions that the original finding was sent to.